cifically tailored to request one or more tokens, e.g. by email, by BT exchange, by SMS, using NFC technology or by using any other suitable communication means known in the art.

**[0082]** However, such a request is optional in that the first client **120** may be equally well initiate provision of the one or more tokens to the second client **140** on its own without an explicit request thereto. In practice it is also possible for the user of the second client **140** to other means to request the one or more tokens from the user of the first client **120**, e.g. by sending an informal request to acquire one or more tokens of desired type(s) e.g. by email, by SMS, etc. or even by a verbal request. Moreover, regardless of the manner of receiving the request to provide the one or more tokens to the second client **140**, the acknowledgement of step **302** may be omitted and the process may move on to the subsequent steps without providing an explicit acknowledgement.

**[0083]** In step **304** of the example of FIG. **9**, the first client **120** obtains the one or more tokens, and in step **306** the first client **120** provides the one or more tokens to the second client **140**. Examples regarding obtaining the token(s) and providing them to the second client **140** are described hereinbefore. Once obtained, the first client **120** may be configured to store the one or more tokens in a memory of the first client **120**, e.g. in a database of other type in order to enable keeping track of the one or more tokens and the identifiers associated therewith. As an example, in case the identifiers associated with the token comprise user identifier(s) of one or more second users, the respective token(s) may be stored as additional entries to a phonebook or a contact list stored in a memory of the first client **120** or the phonebook/contact list may be provided with a pointer to a dedicated table or database in a memory of the first client **120** storing the tokens and identifiers included therein to enable subsequent matching with a received token and associated identifiers.

**[0084]** The first client **120** may be configured to generate and provide only some of the one or more tokens requested by the second client **140** or the user thereof. Such a restriction to refrain from providing all requested tokens to the second client **140** may be based on explicit decision or selection by the user of the first client **120** or to a predefined policy applied in the first client **120**.

**[0085]** Once having the one or more tokens in its disposal, the second client **140** may choose to an appropriate token of the one or more tokens to accompany a communication item to be provided to the first client **120**, as indicated in step **308** of the example of FIG. **9**. In this regard, the user interface of the second client **140** is provided with suitable mechanism(s) that enable the user of the second client **140** to provide a communication item, e.g. a telephone call, an SMS, an MMS, an email message, as described hereinbefore, with a token of his/her choosing. As a non-limiting example in this regard, FIG. **13** schematically illustrates a window or a screen **600** that may be applied to select one of the tokens provided in the portion **610** of the window/screen **600** by ticking the respective box e.g. before selecting and proceeding with initiating one of the communication options **620**.

**[0086]** In step **309** the first client **120** processes the token received together with the communication item to verify the token and/or identifiers associated therewith and in step **310** the first client applies the screening rule to handle or process the incoming communication item in accordance with the identifiers associated with the received token, as described in more detail hereinbefore.

**[0087]** A signaling chart illustrated in FIG. **10** provides a second example of a process for the first client **120** providing the second client **140** with a token and the second client **140**, subsequently, using the token to accompany a communication item addressed to the first client **120**. The steps **401** and **402** of the second example are similar to steps **301** and **302**, respectively, described in context of the (first) example of FIG. **9**.

**[0088]** In optional step **403** of the second example of FIG. **10** the second client **140** provides the first client **120** with an encryption key for subsequent encryption of the one or more tokens. As described hereinbefore, instead of receiving the encryption key from the second client **140**, the first client **120** may generate the encryption key locally or obtain the encryption key from another source.

**[0089]** In step **404** of the second example the one or more tokens are obtained and the token(s) are possibly stored in a memory of the first client, as described in context of step **304** of the (first) example of FIG. **9**. In step **405** the one or more tokens are encrypted and the resulting one or more encrypted tokens may be also stored in a memory of the first client together with their original unencrypted counterparts for subsequent verification purposes. In step **406** the one or more encrypted tokens are provided to one or more second clients **140**, in a manner similar to step **306** of the (first) example of FIG. **9** and described in more detailed examples hereinbefore.

**[0090]** Steps **408** to **410** of the second example correspond to steps **308** to **310** of the (first) example of FIG. **9**, respectively. However, in the second example the verification of the token in step **409** may further comprise decryption the token and the screening rule applied in step **410** may further employ the result of the decryption process in handling of the incoming communication item, as described in more detailed examples hereinbefore.

**[0091]** A signaling chart illustrated in FIG. **11** provides a third example of a process for the first client **120** and two second clients **140**, **140'** applying a token assigned to the user of the second client **140** used to accompany a communication item originating from a further second client **140'**.

**[0092]** In the third example, it is assumed that a token encrypted with an encryption key provided to the first client **120** by the second client **140** or that the encryption key is otherwise provided to disposal of the second client **140**. Such a token may be provided e.g. in accordance with the second example described in context of FIG. **10**.

**[0093]** In step **506** of the third example, which corresponds to the step **406** of the second example, the second client **140** receives one or more encrypted tokens from the first client **120**. In step **507** of the third example, the second client **140** forwards at least one of the encrypted tokens to the further second client **140'**, which may be another user account, another email address, another/new telephone number of the second user, i.e. the user of the second client **140**.

**[0094]** In step **508** the further second client **140'** addresses a communication item to the first client **120** accompanied by the encrypted token and the respective encryption key, thereby enabling the first client **120** to verify that the originator of the communication item indeed is a legitimate user or owner of the encrypted token even though there may not be a match between the source identifier associated with the communication item and any of the user identifiers of the accompanying token. In case the token is associated with user identifiers of a single second user only, the first client **120** may, additionally, conclude that the source identifier of the com-